1/5/5 (Item 5 from file: 351)
DIALOG(R)File 351:Derwent WPI

011570706 **Image available**
WPI Acc No: 1997-547187/ **199750**
XRPX Acc No: N97-456071

WWW gateway system for computer, network - has user management communication unit to communicate with user management control unit which forwards detection request from WWW gateway main body to management unit

Patent Assignee: HITACHI LTD (HITA)
Number of Countries: 001 Number of Patents: 001
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
JP 9265443	A	19971007	JP 9675863	A	19960329	199750	B

Priority Applications (No Type Date): JP 9675863 A 19960329
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
JP 9265443	A		19	G06F-013/00	

Abstract (Basic): JP 9265443 A

The system (7) has an user authentication information table (19) which matches and user authentication information input by a client with an user authentication identifier. The user authentication information is supplied based on an user authentication request. The user authentication information is detected based on detection request. An user authentication information management unit (17) deletes the authentication information which controls the access time for every user. An existing system enquiry unit (18) receives the user authentication information from the management unit. A WWW gateway communication unit (15) communicates with a WWW network. An user authentication request is sent to the existing system inquiry unit based on the user authentication information registration request received from the WWW gateway mainbody through the communication unit. The authentication information identifier acquires the authentication registration request for the management unit.

The authentication information request received from the network through the communication unit is forwarded to the management. An user management controller (13) forwards the deletion request received from the main body through the communication unit according to a communication break request from the user, to the management unit. An user management communication unit (14) communicates with the user management control unit for informing deletion request.

ADVANTAGE - Improves security of user authentication information.

Dwg.1/13

Title Terms: GATEWAY; SYSTEM; COMPUTER; NETWORK; USER; MANAGEMENT; COMMUNICATE; UNIT; COMMUNICATE; USER; MANAGEMENT; CONTROL; UNIT; FORWARD; DETECT; REQUEST; GATEWAY; MAIN; BODY; MANAGEMENT; UNIT
Derwent Class: T01
International Patent Class (Main): G06F-013/00
International Patent Class (Additional): G06F-001/00; G06F-015/00
File Segment: EPI

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号

特開平9－265443

(43)公開日　平成９年(1997)10月７日

(51)Int.Cl.[6]		識別記号	庁内整理番号	Ｆ Ｉ		技術表示箇所
Ｇ０６Ｆ	13/00	３５７		Ｇ０６Ｆ	13/00	３５７Ｚ
	1/00	３７０			1/00	３７０Ｅ
	15/00	３３０			15/00	３３０Ａ

審査請求　未請求　請求項の数３　ＯＬ　（全 19 頁）

(21)出願番号　特願平8－75863

(22)出願日　平成８年(1996)３月29日

(71)出願人　000005108
株式会社日立製作所
東京都千代田区神田駿河台四丁目６番地

(72)発明者　大高　政浩
神奈川県横浜市戸塚区戸塚町5030番地　株式会社日立製作所ソフトウェア開発本部内

(72)発明者　橋本　和広
大阪府大阪市中央区北浜三丁目５番29号　日立西部ソフトウェア株式会社内

(72)発明者　小谷　純一
大阪府大阪市中央区北浜三丁目５番29号　日立西部ソフトウェア株式会社内

(74)代理人　弁理士　小川　勝男

最終頁に続く

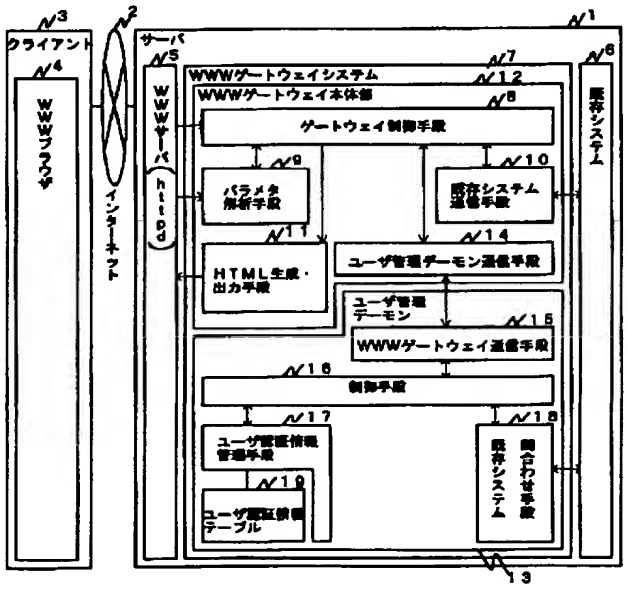
(54)【発明の名称】　WWWゲートウェイシステム

(57)【要約】

【課題】WWWゲートウェイプログラムのユーザ認証情報の画面間の継承がセキュリティホールとなる危険性がある点を解消し、セキュリティとユーザの利便性の両方を確保したユーザ認証によるアクセス権限管理が可能なWWWゲートウェイシステムを提供する。

【解決手段】WWWゲートウェイ本体部１２における画面間のユーザ認証情報の継承をユーザ認証情報識別子をキーにして管理するユーザ認証情報管理手段１７を備える計算機環境に常駐するユーザ管理デーモン１３を有するものである。

図1



1

【特許請求の範囲】

【請求項１】ユーザ認証情報登録要求に対してユーザがクライアントから入力したユーザ認証情報をユーザ認証情報識別子と対応付けて登録したユーザ認証情報テーブルと、ユーザ認証情報要求に対してユーザ認証情報を渡し、ユーザ認証情報削除要求に対し当該ユーザのユーザ認証情報を削除し、WWW（Ｗｏｒｌｄ　ＷｉｄｅＷｅｂ）ゲートウェイシステムに最後にアクセスした時刻をユーザ毎に管理し一定時間が経過したユーザのユーザ認証情報を削除するユーザ認証情報管理手段と、

ユーザ認証要求に対してアクセス対象の既存システムにユーザがクライアントから入力したユーザ認証情報を渡し、ユーザ認証結果を受け取る既存システム問合わせ手段と、

WWWゲートウェイ本体部との通信を行うWWWゲートウェイ通信手段と、

上記WWWゲートウェイ通信手段経由で受け取ったWWWゲートウェイ本体部からのユーザ認証情報登録要求に対して、ユーザ認証要求を上記既存システム問合わせ手段に発行し、その応答により認証成功ならばユーザ認証登録要求を上記ユーザ認証情報管理手段に発行して取得するユーザ認証情報識別子を、認証失敗ならば認証失敗通知を上記WWWゲートウェイ通信手段経由でWWWゲートウェイ本体部に応答し、また上記WWWゲートウェイ通信手段経由で受け取ったWWWゲートウェイ本体部からのユーザ認証情報要求を上記ユーザ認証情報管理手段に転送してその結果を上記WWWゲートウェイ通信手段経由でWWWゲートウェイ本体部に応答し、またユーザの通信断要求に応じて上記WWWゲートウェイ通信手段経由でWWWゲートウェイ本体部から受け取るユーザ認証情報削除要求を上記ユーザ認証情報管理手段に転送してその結果を上記WWWゲートウェイ通信手段経由でWWWゲートウェイ本体部に応答する制御手段を含むユーザ管理デーモンと、

WWWゲートウェイ本体部にユーザ管理デーモンとの通信を行うユーザ管理デーモン通信手段を備えたことを特徴とするWWWゲートウェイシステム。

【請求項２】請求項１に記載のWWWゲートウェイシステムにおいて、上記ユーザ管理デーモンとして、

ユーザ情報テーブルを設け、ユーザ毎の情報を管理し、またWWWゲートウェイ本体部からの要求に対して当該情報を応答し、また上記ユーザ認証情報管理手段がユーザ認証情報を削除するときに当該ユーザのユーザ情報を上記ユーザ情報テーブルから削除するユーザ情報管理手段を備えたことを特徴とするWWWゲートウェイシステム。

【請求項３】請求項１に記載のWWWゲートウェイシステムにおいて、WWWゲートウェイ本体部として、

上記ユーザ管理デーモンにユーザ認証情報要求をした結果、WWWゲートウェイシステムに最後にアクセスした

2

時間から一定時間が経過しておりユーザ認証情報が削除されている通知を受け取った場合に、表示するユーザ認証画面に前回の処理を継続するための情報を埋め込む継続処理情報埋め込み手段を備えたことを特徴とするWWWゲートウェイシステム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、WWW（Ｗｏｒｌｄ　Ｗｉｄｅ　Ｗｅｂ）向けでない既存のシステムとWWWサーバの間を仲介して既存システムをWWWブラウザからアクセス可能にするWWWゲートウェイシステムに係わり、特にユーザ認証によるアクセス管理を行う既存システムに対して、当該システムのアクセス管理をそのまま活用するユーザ認証の手段を備えるWWWゲートウェイシステムに関する。

【０００２】

【従来の技術】インターネット上に分散している資源を統一的にハイパーテキスト形式で参照（ブラウジング）するためのシステムであるWWWは、広域的な情報基盤として注目されている。このWWWを活用して既存のシステムに蓄積されている情報を全世界的に発信することを目的とした、既存システムとWWWサーバの間を仲介するゲートウェイプログラムの開発が盛んになっている（”特集／アプリケーション連携－業務プログラムもWWWで”、日経コミュニケーション１２月１８日号、第２１２号、１９９５年、１３６頁～１４０頁）。

【０００３】WWWゲートウェイシステムは、ＣＧＩ（Ｃｏｍｍｏｎ　Ｇａｔｅｗａｙ　Ｉｎｔｅｒｆａｃｅ）スクリプトとして開発するのが一般的である。ＣＧＩはWWWサーバとサーバ上で動く他のプログラムやスクリプトとのインタフェースの役割を果たす（ローラ・リメイ：”続・ＨＴＭＬ入門－新機能、ＣＧＩ、Ｗｅｂの進化”、プレンティスホール出版、１９９５年）。

【０００４】図２は従来のWWWゲートウェイシステムの構成を説明する図である。図２において、１はサーバ、３はクライアントであり、サーバ１とクライアント３はインターネット２で接続されている。サーバ１上ではWWWサーバ５（ｈｔｔｐｄ：ＨｙｐｅｒＴｅｘｔ　Ｔｒａｎｓｆｅｒ　Ｐｒｏｔｏｃｏｌ　Ｄａｅｍｏｎ）を、クライアント３上ではWWWブラウザ４を動作させることにより、WWWによる情報発信および受信が可能になる。WWWゲートウェイシステム７は、WWWサーバ５から起動され、WWWサーバ５と既存システム６の仲介をする。

【０００５】WWWゲートウェイシステム７は、WWWサーバ５からのデータの受信ならびにデータの解析を行うパラメタ解析手段９と、既存システム６とのインタフェースとなる既存システム通信手段１０と、処理結果からWWWサーバ５向けの画面データ記述形式であるＨＴＭＬ（ＨｙｐｅｒＴｅｘｔ　Ｍａｒｋｕｐ　Ｌａｎｇｕ

ａｇｅ）形式で画面出力データを生成しWWWサーバ５に出力するＨＴＭＬ生成・出力手段１１と、それらを制御するゲートウェイ制御手段８より構成される。ユーザからの処理要求をWWWブラウザ４からインターネット２経由で受け取ったWWWサーバ５は、それがWWWゲートウェイシステム７への処理要求ならばWWWゲートウェイシステム７を起動する。WWWゲートウェイシステム７では、パラメタ解析手段９がWWWサーバ５からデータを受け取り、解析し、それを基にゲートウェイ制御手段８が既存システム通信手段１０を経由して既存システム６を操作して処理を行い、その結果をＨＴＭＬ生成・出力手段１１によりＨＴＭＬ形式の画面データにしてWWWサーバ５に出力する。WWWサーバ５は、それをインターネット２を経由してクライアント３上のWWWブラウザ４に送信し、WWWブラウザ４がその画面データを表示する。以上のようにして、WWW向けでない既存システムをWWWを使用してアクセスできるようにする。

【０００６】

【発明が解決しようとする課題】既存システムの中にはユーザ認証により情報に対するアクセス権限を管理する機能を持っているものがあり、WWWを通じて情報発信する際にもこのアクセス権限管理を有効にしたいとのニーズがある。そのためには、ゲートウェイプログラムがユーザからユーザＩＤやパスワードといったユーザ認証を行うための情報を入力させ、それを既存システムに渡すことが必要となる。しかし、WWWゲートウェイプログラムはゲートウェイプログラムを実現するＣＧＩの仕様により、ユーザ操作のたびに起動され画面出力処理が終わるとプログラムの動作を終了しなければならず、ユーザの入力したユーザ認証情報に基づいて複数の画面を遷移して操作を行うような処理において、専用のクライアントアプリケーションのように既存システムとのセッションを接続したままにすることや、ユーザ認証情報をメモリ上に保持しつづけることができない。つまり、ユーザ認証情報の画面間の継承が問題となる。

【０００７】この問題に対する一般的な解決方法としては、ＨＴＭＬのｈｉｄｄｅｎタグを使用して画面情報にユーザ認証情報を埋め込む方法と、画面毎に必要に応じてユーザ認証情報を再入力させる方法の２つの方法が考えられる。しかし、前者では、例え画面情報に埋め込んだユーザ認証情報を暗号化したとしても、画面情報のハッキングによりセキュリティホールとなる危険性がある。後者では、ユーザ認証情報を度々入力しなければならず、ユーザの利便性を著しく損なうこととなる。

【０００８】本発明のい目的は、ユーザ認証によるアクセス管理を行う既存システムに対して、ユーザの入力したユーザ認証情報に基づいて複数の画面を遷移して操作を行うような処理において、ユーザ認証情報の画面間の継承を行うことにより、セキュリティとユーザの利便性

（アクセスのたびにユーザ認証情報を入力しなくて良い）の両方を確保したWWWゲートウェイシステムを提供することにある。

【０００９】

【課題を解決するための手段】ユーザ認証情報を計算機環境に常駐するユーザ管理デーモンに管理させ、WWWゲートウェイ本体部（以下では、WWWゲートウェイシステムを従来のWWWゲートウェイシステムとユーザ管理デーモンを統合したものと位置付け、従来のWWWゲートウェイシステムはWWWゲートウェイ本体部と呼ぶ）はそこから取得したユーザ認証情報を使用することにより、前記課題を解決する。ユーザ管理デーモンはユーザ認証情報毎にユニークでかつハッキングのされにくいユーザ認証情報識別子を割り振り、それをWWWゲートウェイ本体部に渡す。WWWゲートウェイ本体部はユーザ認証情報の代わりにユーザ認証情報識別子を画面間で継承し、ユーザ認証情報が必要な場合はユーザ認証情報識別子をキーにユーザ管理デーモンにユーザ認証情報要求を発行してユーザ認証情報を取得する。以上のようにユーザ管理デーモンにユーザ認証情報を管理させることにより、セキュリティとユーザの利便性の両方を確保したユーザ認証情報の画面間の継承が可能となる。

【００１０】ユーザ管理デーモンは、具体的には次の手段で構成する。

【００１１】（１）ユーザ認証情報テーブルを設け、ユーザ認証情報登録要求に対してユーザがクライアントから入力したユーザ認証情報をユーザ認証情報識別子と対応付けて登録し、またユーザ認証情報要求に対してユーザ認証情報を渡し、またユーザ認証情報削除要求に対し当該ユーザのユーザ認証情報を削除し、またWWWゲートウェイシステムに最後にアクセスした時刻をユーザ毎に管理し一定時間が経過したユーザのユーザ認証情報を削除するユーザ認証情報管理手段

（２）ユーザ認証要求に対してアクセス対象の既存システムにユーザがクライアントから入力したユーザ認証情報を渡し、ユーザ認証結果を受け取る既存システム問合わせ手段

（３）WWWゲートウェイ本体部との通信を行うWWWゲートウェイ通信手段

（４）上記WWWゲートウェイ通信手段経由で受け取ったWWWゲートウェイ本体部からのユーザ認証情報登録要求に対して、ユーザ認証要求を上記既存システム問合わせ手段に発行し、その応答により認証成功ならばユーザ認証登録要求を上記ユーザ認証情報管理手段に発行して取得するユーザ認証情報識別子を、認証失敗ならば認証失敗通知を上記WWWゲートウェイ通信手段経由でWWWゲートウェイ本体部に応答し、また上記WWWゲートウェイ通信手段経由で受け取ったWWWゲートウェイ本体部からのユーザ認証情報要求を上記ユーザ認証情報管理手段に転送してその結果を上記WWWゲートウェイ

通信手段経由でWWWゲートウェイ本体部に応答し、またユーザの通信断要求に応じて上記WWWゲートウェイ通信手段経由でWWWゲートウェイ本体部から受け取るユーザ認証情報削除要求を上記ユーザ認証情報管理手段に転送してその結果を上記WWWゲートウェイ通信手段経由でWWWゲートウェイ本体部に応答する制御手段

また、WWWゲートウェイ本体部にもユーザ管理デーモンとの通信を行うユーザ管理デーモン通信手段を追加する。

【００１２】これらの手段をWWWゲートウェイシステムに付加し、ユーザ管理デーモンを計算機環境に常駐させることにより、ユーザ認証情報はユーザ管理デーモンの作業メモリ上に管理し、画面間のユーザ認証情報の継承はユーザがWWWゲートウェイシステムへのアクセスを開始するたびに設定されるユーザ認証情報識別子により行われるようになり、セキュリティとユーザの利便性の両方を確保したユーザ認証情報の画面間の継承が可能となる。

【００１３】

【発明の実施の形態】以下、本発明の実施の形態について例を上げて詳細に説明する。

【００１４】まず第１の実施例について説明する。

【００１５】図１は本実施例の構成を示すブロック図である。図１において、１はサーバ、２はインターネット、３はクライアント、４はWWWブラウザ、５はWWWサーバ、６は既存システム、７はWWWゲートウェイシステムである。ここで、WWWゲートウェイシステム７は、WWWゲートウェイ本体部１２とユーザ管理デーモン１３よりなる。

【００１６】WWWゲートウェイ本体部１２は、WWWサーバ５から起動される部分である。WWWゲートウェイ本体部の実装には、WWWサーバ５とのインタフェースを提供するＣＧＩを導入しても良い。WWWゲートウェイ本体部１２は、WWWブラウザ４上でユーザがした画面操作（例えばボタン押下やアンカークリック）に対してWWWサーバ５により起動され、一連の処理を行った後、画面データをWWWサーバ５に対して出力して動作を終了する。一方、ユーザ管理デーモン１３はWWWゲートウェイ本体部１２が起動される前にシステム管理者が起動し、システム管理者が明示的に停止させるまで計算機環境上に常駐し続ける。そしてWWWゲートウェイ本体部１２からの処理要求を受け、それに対して応答する。

【００１７】WWWゲートウェイ本体部１２は、従来のWWWゲートウェイの要素であるゲートウェイ制御手段８と、パラメタ解析手段９と、既存システム通信手段１０と、ＨＴＭＬ生成・出力手段１１と、それに加えてユーザ管理デーモン通信手段１４より構成する。ユーザ管理デーモン通信手段１４は、ゲートウェイ制御手段８からの通信処理要求に対してユーザ管理デーモン１３に発行するメッセージを生成して発行し、またユーザ管理デーモン１３から受け取った応答をゲートウェイ制御手段８で処理できるかたちに変換する機能を持つ。

【００１８】ユーザ管理デーモン１３は、WWWゲートウェイ本体部１２との通信を制御するWWWゲートウェイ通信手段１５と、ユーザ認証情報を格納するユーザ認証情報テーブル１９と、ユーザ認証情報テーブル１９を管理するユーザ認証情報管理手段１７と、既存システム６に対してユーザ認証の判定要求を発行する既存システム問合わせ手段１８と、以上のユーザ管理デーモン１３の構成要素を制御する制御手段１６より構成する。

【００１９】ここでユーザ認証情報テーブル１９に格納するユーザ認証情報とは、既存システム６がユーザ認証を行うために要求する情報であり、例えば各ユーザ毎に割り振られたユーザＩＤやパスワードであってもよい。

【００２０】図３は、ユーザ認証情報テーブル１９の例を説明するための図である。この例ではユーザ認証のための情報として、ユーザＩＤとパスワードとＩＰアドレスを使用している。これらのユーザ認証情報にアクセスするためのキーとして各情報にユーザ認証情報識別子を付加する。ユーザ認証情報識別子は、ユーザ認証情報を取得するためのキーとして使用されるため、ユニークでなければならない。また、WWWゲートウェイ本体部１２に渡され、画面情報に埋め込んで継承されるため、盗用される恐れのないものでなければならない。例えば、当該ユーザのユーザＩＤと、当該ユーザがWWWゲートウェイシステム７の操作を開始した日時と、起動されたWWWゲートウェイ本体部１２のプロセスＩＤについて、末尾を予め定めたサイズだけ切り出して連結し、それを予め定めた手順で暗号化して生成した文字列をユーザ認証情報識別子として使用しても良い。ユーザ認証情報テーブル１９はさらに当該ユーザが最後にWWWゲートウェイシステム７にアクセスした時刻を格納するフィールドも含む。これは、WWWゲートウェイシステム７に一定時間アクセスがなかった場合に当該ユーザの認証情報を削除する処理（タイムアウト処理）で使用される。

【００２１】なお、ユーザ認証情報テーブル１９をファイルとして管理するとそれを参照して盗用される恐れがあるため、ユーザ認証情報テーブル１９はユーザ管理デーモン１３が管理する作業メモリ上に管理する。

【００２２】図１の構成のWWWゲートウェイシステム７でユーザの操作に対する処理の流れを次に説明する。

【００２３】ユーザがWWWゲートウェイシステム７にアクセスすると、WWWゲートウェイシステム７はまずユーザ認証情報を入力するための画面（以下ではユーザ認証画面と呼ぶ）を表示してユーザにユーザ認証情報の入力を促す。WWWゲートウェイシステム７を使用して既存システム６にアクセスするためには、ユーザはまずユーザ認証画面でユーザ認証情報を入力しなければなら

ない。図４にユーザがユーザ認証画面でユーザ認証情報を入力したとき（この操作を以下ではログインと呼ぶ）のWWWゲートウェイシステム７の処理の流れを示す。

【００２４】ユーザがログインをするとWWWサーバ５がWWWゲートウェイ本体部１２を起動する。WWWゲートウェイ本体部１２ではゲートウェイ制御手段８が処理１０１においてパラメタ解析手段９にパラメタ解析要求２０１を発行する。パラメタ解析手段９は、処理１０２においてWWWサーバ５からパラメタを入力しそれを解析してゲートウェイ制御手段８に応答する（２０２）。パラメタ解析結果２０２を受け取ったゲートウェイ制御手段８は、解析結果からユーザの操作がユーザ認証情報入力であることを判断して、処理１０３においてユーザ認証要求２０３をユーザ管理デーモン通信手段１４に発行する。ユーザ管理デーモン通信手段１４は、処理１０４においてユーザ認証要求２０３をユーザ管理デーモン１３に対するメッセージ２０４に変換し、それをユーザ管理デーモン１３に発行する。そしてユーザ管理デーモン１３からの応答待機状態に遷移する。

【００２５】ユーザ管理デーモン通信手段１４が発行したメッセージ２０４はユーザ管理デーモン１３の中のWWWゲートウェイ通信手段１５が受け取る。WWWゲートウェイ通信手段１５は処理１０５において受け取ったメッセージ２０４を解析しその結果を制御手段１６に送信する（２０５）。メッセージ解析結果２０５を受け取った制御手段１６は、処理１０６において解析結果からユーザ認証情報を取り出しそれをもとにユーザ認証要求２０６を既存システム問合わせ手段１８に発行する。ユーザ認証要求２０６を受け取った既存システム問合わせ手段１８は、処理１０７においてそれを既存システム６向けの処理要求２０７にして既存システム６へ発行する。既存システム６は受け取ったユーザ認証情報からユーザ認証を行い、当該ユーザが既存システム６にアクセスできるかどうかの判定結果を既存システム問合わせ手段１８に応答する（２０８）。このように、ユーザ認証画面を表示しユーザ認証情報を受け取るのはWWWゲートウェイシステム７だが、WWWゲートウェイシステム７自体がアクセス権限管理を行うわけでなく、既存システム６にユーザ認証情報を渡して既存システム６がユーザ認証によるアクセス権限管理を行う。

【００２６】既存システム６からユーザ認証結果２０８を受信した既存システム問合わせ手段１８は、処理１０８においてそのユーザ認証結果２０９を制御手段１６に応答する。制御手段１６は、処理１０９において認証結果２０９の判定を行う。もし当該ユーザが既存システム６にアクセス可能であるという認証結果ならば、そのユーザ認証情報をユーザ認証情報テーブル１９に登録するようユーザ認証情報管理手段１７に処理要求２１０を発行する。ユーザ認証情報登録要求２１０を受けたユーザ認証情報管理手段１７は、まず処理１１０でユーザ認証情報識別子を生成する。ユーザ認証情報識別子の生成には上記で説明した、WWWゲートウェイ本体部１２からのメッセージで渡されるユーザＩＤやプロセスＩＤ、ユーザ管理デーモンが独自に取得する操作開始時刻を結合し暗号化する方法を使用してもよい。　処理１１０でユーザ認証情報識別子を生成した後、処理１１１でそのユーザ認証情報識別子とユーザ認証情報、およびアクセス時刻をユーザ認証情報テーブル１９に格納する。ユーザ認証情報管理手段１７は、当該ユーザ認証情報をユーザ認証情報テーブル１９に格納した後、制御手段１６にユーザ認証情報識別子を応答する（２１１）。応答２１１を受け取った制御手段１６は処理１１２としてユーザ認証情報識別子をWWWゲートウェイ本体部１２に応答するようWWWゲートウェイ通信手段１５に処理要求を発行する（２１２）。

【００２７】一方、処理１０９で当該ユーザが既存システム６にアクセスできないという認証結果ならば、制御手段１６は上記の処理１１０と処理１１１のユーザ認証情報の登録は行わず、処理１１２においてユーザ認証に失敗した旨をWWWゲートウェイ本体部１２に応答するようWWWゲートウェイ通信手段１５に処理要求を発行する（２１２）。

【００２８】WWWゲートウェイ通信手段１５は、処理１１３において制御手段１６から受け取った処理結果をWWWゲートウェイ本体部１２に発信するメッセージ２１３に変換し、それをWWWゲートウェイ本体部１２に発信する。以上でユーザ管理デーモン１３の一連の処理は終了するが、ユーザ管理デーモン１３は動作を停止せずに、計算機環境に常駐しWWWゲートウェイ本体部１２からの処理要求待機状態に遷移する。

【００２９】WWWゲートウェイ通信手段１５が発行したメッセージは、ユーザ管理デーモン１３からの応答待機状態にあったユーザ管理デーモン通信手段１４が受け取り、処理１１４においてそれを解析してゲートウェイ制御手段８に送信する（２１４）。メッセージ解析結果２１４を受け取ったゲートウェイ制御手段８は、処理１１５においてユーザ認証結果を表示する画面情報（ＨＴＭＬ形式）の出力要求２１５をＨＴＭＬ生成・出力手段１１に発行する。このとき、ユーザ管理デーモン１３から受け取ったユーザ認証結果がユーザ認証成功、すなわちユーザ認証情報識別子ならばそれを埋め込んだシステムの初期画面の画面情報の生成を指示し、ユーザ認証失敗通知ならばユーザ認証に失敗したことをユーザに通知し再度ユーザ認証情報を入力させるための画面情報の生成を指示する。

【００３０】画面情報の出力要求２１５を受け取ったＨＴＭＬ生成・出力手段１１は、まず処理１１６において画面情報を生成し、その画面情報を処理１１７においてWWWサーバ５に出力する（２１６）。ユーザ認証情報識別子の画面情報への埋め込みには、ＨＴＭＬのｈｉｄ

ｄｅｎタグを使用する方法を採用する。以上でWWWゲートウェイ本体部１２の一連の処理が終了し、WWWゲートウェイ本体部１２は動作を停止する。

【００３１】ユーザがログインすると、WWWゲートウェイシステム７では既存システム６に当該ユーザ認証情報を渡してユーザ認証によるアクセス権限の確認を行わせた後、もし当該ユーザが既存システム６にアクセス可能ならば、当該ユーザ認証情報をユーザ管理デーモン１３のユーザ認証情報テーブル１９に登録する。そして、ユーザ認証情報テーブル１９から当該ユーザ認証情報を取り出すためのキーとなるユーザ認証情報識別子をWWWゲートウェイ本体部１２が出力する画面情報に埋め込み画面間のユーザ認証情報の継承を行う。

【００３２】次に画面情報に埋め込まれたユーザ認証情報識別子を基にユーザ認証情報を取得し既存システム６にアクセスするときの処理の流れを説明する。

【００３３】図５は、WWWゲートウェイシステム７からユーザ認証の必要な既存システム６の処理を実行するときの処理の流れを説明する図である。

【００３４】上記と同様にパラメタ解析手段９の解析結果２０２を受け取ったゲートウェイ制御手段８が、解析結果２０２を基にWWWゲートウェイ本体部１２の実行すべき処理を決定する。本実施例では、ユーザ認証の必要な既存システム６の処理を実行するものとすると、ゲートウェイ制御手段８はまず前画面に埋め込まれていたユーザ認証情報識別子をパラメタ解析手段９の解析結果から取り出し、それをキーにしてユーザ管理デーモン１３からユーザ認証情報を取得する。そのために処理１２１において、ユーザ認証情報要求２２１をユーザ管理デーモン通信手段１４に送信する。

【００３５】ユーザ管理デーモン通信手段１４では上記と同様にゲートウエイ制御手段８から受けたユーザ管理デーモン１３への処理要求２２１をメッセージ２０４に変換し、ユーザ管理デーモン１３に発信する。ユーザ管理デーモン１３では、WWWゲートウェイ通信手段１５が当該メッセージを受信し、解析を行ない、その結果２０５を制御手段１６に送信する。制御手段１６は、処理１２２において解析結果２０５からユーザ認証情報識別子を取り出し、それをキーにして求めるユーザ認証情報を検索するよう、ユーザ認証情報管理手段１７にユーザ認証情報要求２２２を送信する。ユーザ認証情報管理手段１７は、処理１２３においてユーザ認証情報要求２２２からユーザ認証情報識別子を取り出し、それをキーにしてユーザ認証情報テーブル１９の検索を実行する。

【００３６】例えば、図３のユーザ認証情報テーブル１９の例において、ユーザ認証情報識別子ＫＵＩ０３８９０Ｖ９３が与えられたとすると、それに対するユーザ認証情報として、ユーザＩＤ：ＡＩＫＯＵ、パスワード：ＺＺＺ＆＆（）＠、ＩＰアドレス：１２３．４５．６７．１２３を取得する。この際、テーブルにアクセスした時刻で最終アクセス時間のフィールドを置き換える。例えば、テーブルにアクセスした時刻が９６０３０８１７３２４７だとすると、現在登録されている最終アクセス時刻：９６０３０８１５４５１７を９６０３０８１７３２４７に置き換える。取得したユーザ認証情報を制御手段１６に応答する（２２３）。なお、ユーザ認証情報管理手段１７において当該ユーザ認証情報識別子に対応した情報がユーザ認証情報テーブル１９に存在しない場合は、エラーを出力する。

【００３７】ユーザ認証情報を受け取った制御手段１６は、上記の例と同様にその結果をWWWゲートウェイ通信手段１５経由でWWWゲートウェイ本体部１２に応答し、応答メッセージを受け取ったユーザ管理デーモン通信手段１４がそれを解析してWWWゲートウェイ制御手段８に渡す。

【００３８】ユーザ管理デーモン１３からのメッセージの解析結果としてユーザ認証情報を受け取ったゲートウェイ制御手段８は、それを付加した既存システム６への処理要求２２４を既存システム通信手段１０に発行する。処理要求２２４を受け取った既存システム通信手段１０は、処理１２５において既存システム６向けの処理要求２２５を生成して発行する。処理要求２２５を受け取った既存システム６は、処理要求２２５に含まれたユーザ認証情報によるアクセス権限に基づいた処理を実行しその結果をWWWゲートウェイ本体部１２に応答する。以降は従来のWWWゲートウェイシステムと同様に処理結果からＨＴＭＬ形式の画面情報を生成し、それをWWWサーバ５に出力して一連の処理を終了する。ただし、出力する画面情報にはユーザ認証情報識別子を継承する。

【００３９】以上のように、画面情報の中にユーザ認証情報識別子を埋め込み、それをWWWゲートウェイ本体部１２のパラメタ解析手段９により取り出し、それをキーにしてユーザ管理デーモン１３のユーザ認証情報管理手段１７から当該ユーザのユーザ認証情報を取得し、それに基づいた処理依頼を既存システム６にすることにより、WWWゲートウェイシステム７からユーザ認証の必要な既存システム６の処理を実行することが可能となる。処理の実行結果として出力する画面情報に、またユーザ認証情報識別子を埋め込むことにより、次のWWWゲートウェイシステム７の起動にユーザ認証情報を継承することができる。

【００４０】以上のようにしてユーザ管理デーモン１３の中のユーザ認証情報テーブル１９にユーザ認証情報を蓄積し、それにユーザ認証情報識別子をキーにしてアクセスすることにより画面間でユーザ認証情報を継承する。しかし、ユーザ認証情報を格納しつづけるとユーザ認証情報テーブル１９のメモリサイズが増大し、ひいては計算機環境のリソース不足を招くことになる。よって、ユーザ認証情報テーブル１９からユーザ認証情報を

削除する処理が必要となる。ユーザ認証情報テーブル１９からユーザ認証情報を削除する手順として、次に２つの手順を説明する。

【００４１】第１の手順は、ユーザから明示的にWWWゲートウェイシステム７の利用終了を通知させる（以下ではこの操作をログアウトと呼ぶ）ものである。画面にユーザがログアウトするための部品を用意し、それに対して操作されたときにユーザ認証情報管理手段１７がユーザ認証情報テーブル１９から当該ユーザのユーザ認証情報を削除する。

【００４２】しかし、第１の手順だけでは、ユーザがログアウトし忘れた場合などにユーザ認証情報がユーザ認証情報テーブル１９に残ったままになってしまう。WWWブラウザ４は、表示した画面をキャッシュしておき、画面操作でWWWブラウザ４起動時から表示してきた画面を順次再表示する機能を持っている。ユーザがWWWブラウザ４でハイパーリンクをたどって次々に画面遷移していくうちに、WWWゲートウェイシステム７をログアウトし忘れることが起こり得るが、このとき第３者が上記の画面キャッシュの機能により、WWWゲートウェイシステム７の画面を再表示し操作すると、ユーザ認証に必要なユーザ認証情報識別子が画面に埋め込まれているため、当該ユーザの権限で第３者の不正な操作を受け付けてしまうこととなる（ログアウト後は、既にユーザ認証情報識別子に対応したユーザ認証情報テーブル１９の項目が削除されているため、画面キャッシュの機能でゲートウェイシステム７の画面を再表示し操作しても有効にならない）。

【００４３】こうした問題を軽減する第２の手順として、ユーザがWWWゲートウェイシステム７に最後にアクセスした時刻から予め定められた時間が経過したユーザの認証情報をユーザ認証情報テーブル１９から削除する（こうしたユーザ管理デーモン１３の処理を以下ではタイムアウト処理と呼ぶ）。図３の例に示した通り、ユーザ認証情報テーブル１９の各項目に対して最終アクセス時刻を設定するフィールドを用意する。

【００４４】上記の説明でも触れたとおり、WWWゲートウェイシステム７にアクセスするたびにユーザ管理デーモン１３のユーザ認証情報管理手段１７が当該ユーザの最終アクセス時刻を更新する。ユーザ認証情報管理手段１７は、最終アクセス時刻を監視し、アクセスされないまま最終アクセス時刻から予め定義された時間が経過した項目を自動的に削除する。こうすることにより、ユーザがログアウトし忘れた場合にユーザ認証情報がユーザ認証情報テーブル１９に残ってしまうという問題を解消できる。タイムアウト処理によりユーザ認証情報を削除されたユーザがWWWゲートウェイシステム７にアクセスした場合には、再度ユーザ認証画面を表示しユーザ認証情報を入力させる。

【００４５】以上のように、ユーザの操作によりWWWサーバ５から起動され、一連の処理が終了した時点で動作を停止するWWWゲートウェイ本体部１２に対して、システム管理者が起動し計算機環境に常駐し続けるユーザ管理デーモン１３にユーザ認証情報を管理させ、WWWゲートウェイ本体部１２は画面情報に埋め込まれたユーザ認証情報識別子をキーとしてユーザ認証情報を取得することにより、画面間でユーザ認証情報を継承でき、またユーザ認証情報識別子としてユニークでかつハッキングしにくいＩＤを定義することで、セキュリティとユーザの利便性の両方が高いアクセス権限管理の可能なWWWゲートウェイシステムを実現することが可能となる。

【００４６】また、ユーザがログアウトにより明示的にWWWゲートウェイシステムの利用終了を通知したときに当該ユーザのユーザ認証情報をユーザ認証情報テーブルから削除する手順と、ユーザ管理デーモンが最終アクセス時刻からの経過時間を監視し、タイムアウト処理で一定時間アクセスのなかったユーザのユーザ認証情報をユーザ認証情報テーブルから削除する手順を用意することにより、ユーザ認証情報の追加登録によるユーザ認証情報テーブルの肥大化とWWWブラウザの画面キャッシュ機能を悪用した第３者による既存システムへの不正アクセスを防止することが可能となる。

【００４７】次に第２の実施例について説明する。

【００４８】上記第１の実施例では、ユーザ管理デーモンはユーザ認証情報のみを管理した。しかし、ユーザ管理デーモンにその他の情報を管理させることも可能である。ユーザ管理デーモンに管理させることが有効な情報としては、ユーザ毎に管理すべき情報であり、かつ画面間で継承する必要がある情報があげられる。

【００４９】例としては、既存システムに渡すべきコンフィギュレーションパラメタなどが考えられる。画面間で継承する必要がある情報は通常画面情報に埋め込んで継承するが、WWWブラウザで参照できてしまう画面情報に埋め込むことがセキュリティの観点から適切でない情報の継承に特に有効である。

【００５０】図６は本実施例の構成を示すブロック図である。図において、ユーザ管理デーモン１３にユーザ毎に追加情報を格納するユーザ情報テーブル２１とそれを管理するユーザ情報管理手段２０を追加する。

【００５１】図７は本実施例におけるユーザ認証情報テーブル１９の例である。各ユーザ毎にユーザ情報テーブルへのアドレスを格納するためのフィールドを追加している。　図８は本実施例におけるユーザ情報テーブル２１の例である。ユーザ認証情報テーブル１９に登録されたアドレスに既存システム６に渡すコンフィギュレーションパラメタが２つ格納されている。

【００５２】図９で本実施例におけるログイン時のWWWゲートウェイシステム７の処理の流れを説明する。ユーザ管理デーモン１３の既存システム問合わせ手段１８

の結果に対して制御手段１６で認証結果判定１０９を行うまでの処理は、第１の実施例におけるログイン時の処理（図４）と同じである。また、認証結果判定１０９で認証失敗と判定した場合の以降の処理もまた第１の実施例におけるログイン時の処理と同じである。認証結果判定１０９において認証成功と判定した場合、既存システム問合わせ手段１８に対してユーザ情報要求２３１を発行する。既存システム問合わせ手段１８は、処理１３１においてそれを既存システム向けのユーザ情報要求２３２に変換して発行する。既存システム６ではユーザ情報を検索してそれを応答する（２３３）。既存システム６からユーザ情報の応答２３３を受けた既存システム問合わせ手段１８は、処理１３２においてそれを制御手段１６に応答する（２３４）。

【００５３】既存システム問合わせ手段１８からの応答２３４を受け取った制御手段１６は、処理１３３においてそのユーザ情報の登録要求２３５をユーザ情報管理手段２０に発行する。ユーザ情報登録要求２３５を受け取ったユーザ情報管理手段２０は、処理１３４においてそれをユーザ情報テーブル２１に登録し、その項目のアドレスを制御手段１６に応答する（２３６）。ユーザ情報テーブル２１の当該ユーザ情報を格納した項目のアドレスを受け取った制御手段１６は、処理１３５においてそのアドレスとユーザ認証情報をユーザ認証情報登録要求２３７としてユーザ認証情報管理手段１７に発行する。ユーザ認証情報登録要求２３７を受け取ったユーザ認証情報管理手段１７は、まず処理１１０においてユーザ認証情報識別子を生成し、処理１３６においてそれとユーザ認証情報とアクセス時刻とユーザ情報テーブルアドレスとをユーザ認証情報テーブル１９に格納する。それ以降の処理は第１の実施例のログイン時の処理の流れと同じである。

【００５４】以上のようにしてログイン時にユーザ情報を登録する。次に以上のようにして登録したユーザ情報を使用する際の処理の流れをユーザ情報取得の処理の流れを説明する図である図１０を用いて説明する。

【００５５】まずWWWゲートウェイ本体部１２のゲートウェイ制御手段８から、処理１４１においてユーザ情報要求２４１が発行される。ユーザ情報要求２４１はユーザ管理デーモン通信手段１４の処理１０４においてユーザ管理デーモン１３へのメッセージ２０４に変換され発行される。メッセージ２０４はユーザ管理デーモン１３のWWWゲートウェイ通信手段１５の処理１０５において受信、解釈されて制御手段１６に転送される（２４２）。制御手段１６では、まず処理１４２においてメッセージ解析結果２４２からユーザ認証情報識別子を切り出し、それを基にユーザ情報テーブルアドレス要求２４３をユーザ認証情報管理手段１７に発行する。ユーザ認証情報管理手段１７は、処理１４３においてユーザ情報テーブルアドレス要求２４３に含まれるユーザ認証情報識別子をキーにユーザ認証情報テーブル１９から当該ユーザのユーザ情報テーブルアドレスを取得し、それを制御手段１６に応答する（２４４）。

【００５６】例えば、図７のユーザ認証テーブル１９の例において、ユーザ認証情報識別子としてＫＵＩ０３８９０Ｖ０９３が与えられたとすると、それに対応したユーザ情報テーブルアドレス：６Ｂ７Ｃ１１４０が応答される。制御手段１６は、処理１４４において応答２４４からユーザ情報テーブルアドレスを切り出しユーザ情報要求２４５を生成して、それをユーザ情報管理手段２０に発行する。ユーザ情報要求２４５を受け取ったユーザ情報管理手段２０は処理１４５においてユーザ情報テーブルアドレスを基にユーザ情報テーブル２１からユーザ情報を取得し、それを制御手段１６に応答する（２４６）。

【００５７】例えば図８のユーザ情報テーブル２１の例において、ユーザ情報テーブルアドレス：６Ｂ７Ｃ１１４０に対応したパラメタ１：ＹＹＹとパラメタ２：ＤＥＦが応答される。応答２４６を受け取った制御手段１６はそれをWWWゲートウェイ通信手段１５とWWWゲートウェイ本体部１２のユーザ管理デーモン通信手段１４を経由してゲートウェイ制御手段８に応答する。以上によりWWWゲートウェイ本体部１２でユーザ情報を取得でき、以降でユーザ情報を使った処理を実行できる。

【００５８】ログアウト時およびタイムアウト時にユーザ認証情報テーブル１９の当該ユーザの項目が削除されるタイミングで、ユーザ情報テーブル２１の当該ユーザの項目も削除する。

【００５９】以上のようにユーザ管理デーモン１３にユーザ情報テーブル２１を設けそこにユーザ固有の追加情報を格納して、ユーザ情報管理手段２０でそれを管理することにより、画面間でユーザ固有の追加情報を継承することが可能となる。これは、画面情報に埋め込んで継承した場合、WWWブラウザ４の機能により埋め込んだ情報が参照できてしまうためセキュリティ上問題があるようなユーザ情報の継承において特に有効である。

【００６０】次に第３の実施例について説明する。

【００６１】第１の実施例において、タイムアウトによってユーザ認証情報テーブルから登録を削除されたユーザがWWWゲートウェイシステムにアクセスしたとき、WWWゲートウェイシステムは当該ユーザにタイムアウトで登録が削除されていることを通知し、再ログインするためにユーザ認証画面を表示する。しかし、この手順で再ログインすると当該ユーザがタイムアウト以前に行ってきた操作は全て無効になり、もう一度最初から操作を繰り返さなければならないという問題がある。　そこで本実施例では、タイムアウト時に表示するユーザ認証画面の画面情報に当該ユーザがタイムアウト前の操作を継続するための情報（以下では継続処理情報と呼ぶ）を埋め込むことで、ユーザ認証画面から再ログインすると

タイムアウト前の操作以降の処理を継続して行うことができるWWWゲートウェイシステムについて説明する。

【0062】図11は本実施例の構成を示すブロック図である。図において、WWWゲートウェイ本体部12に継続処理情報埋め込み手段22を追加する。

【0063】本実施例の処理ではまず当該ユーザのユーザ認証情報識別子がユーザ認証情報テーブルになかった場合の再ログインのためのユーザ認証画面に継続処理情報を埋め込む処理を行っておき、再ログインのためのユーザ認証画面からユーザ認証情報を入力し認証に成功した後、継続処理情報に従って処理を継続する。

【0064】図12は本実施例における再ログインのためのユーザ認証画面生成処理の流れを説明するための図である。第1の実施例で説明した既存システムの処理をWWWゲートウェイシステム7から行うときの処理（図5）において、ユーザ認証情報管理手段17の処理123で、ユーザ認証情報識別子に対応したユーザ認証情報がユーザ認証情報テーブル19に存在しない場合、ユーザ認証情報管理手段17はエラーを制御手段16に渡し、制御手段16はそれをWWWゲートウェイ通信手段15とWWWゲートウェイ本体部12のユーザ管理デーモン通信手段14を経由してゲートウェイ制御手段8に応答する（251）。エラー応答251を受けたゲートウェイ制御手段8は、処理151において再ログインのためのユーザ認証画面の出力要求252を発行する。

【0065】第1の実施例のシステムでは再ログインのためのユーザ認証画面出力要求252を他の画面出力要求と同様にHTML生成・出力手段11が処理する。それに対して本実施例では、再ログインのためのユーザ認証画面出力要求252は、まず継続処理情報埋め込み手段22が処理する。再ログインのためのユーザ認証画面出力要求252を受け取った継続処理情報埋め込み手段22は、処理152において今回ユーザが行おうとした操作に関するパラメタ（パラメタ解析手段9が解析したもの）を画面情報に埋め込める形にしてそれをHTML生成・出力手段11に渡す（253）。画面情報に埋め込める形としては、HTMLのｈｉｄｄｅｎタグを使用する。

【0066】HTML生成・出力手段11は、処理116において継続処理情報253を埋め込んだ画面情報を生成し、処理117においてそれをWWWサーバ5に出力する。以上の手順でタイムアウト前の操作を継続するための継続処理情報を埋め込んだ再ログインのためのユーザ認証画面を表示する。

【0067】次に再ログインのためのユーザ認証画面でユーザがログインしたときの処理の流れを図13を用いて説明する。第1の実施例で説明したログイン時の処理（図4）において、ユーザ認証情報管理手段17がユーザ認証情報をユーザ認証情報テーブルに格納し、その結果としてユーザ認証情報識別子を制御手段16に応答する。ユーザ認証情報識別子を受け取った制御手段16は、それをWWWゲートウェイ通信手段15とWWWゲートウェイ本体部12のユーザ管理デーモン通信手段14を経由してゲートウェイ制御手段8に応答する。ユーザ認証識別子を受け取ったゲートウェイ制御手段8は、処理124において再ログインのためのユーザ認証画面に埋め込まれていた継続処理情報を基に既存システム6に処理要求224を発行する。処理要求224は、既存システム通信手段10が処理125において既存システム6向けの処理要求225に変換して既存システム6に発行する。以下、既存システム6で処理を実行した以降の処理の流れは、従来のWWWゲートウェイシステムと同様である。

【0068】以上のように、WWWゲートウェイ本体部12に継続処理情報埋め込み手段22を追加して再ログインのためのユーザ認証画面の画面情報に継続処理情報を埋め込み、再ログイン時の処理のユーザ認証情報のユーザ認証情報テーブル19への格納後にその継続処理情報に従った処理を実行することにより、タイムアウトによってユーザ認証情報テーブルから登録を削除されたユーザがWWWゲートウェイシステムにアクセスしたとき、最初から処理をやり直すことなく、タイムアウト前の処理を継続することが可能となる。

【0069】

【発明の効果】ユーザ認証によるアクセス管理を行う既存システムに対するWWWゲートウェイシステムに関して、ユーザ認証情報を計算機環境に常駐しているユーザ管理デーモンに管理させ、WWWゲートウェイ本体部はそこから取得したユーザ認証情報を既存システムに渡すことにより、既存システムのアクセス管理をそのまま活用したユーザ認証を行うことが可能となる。その際、ユーザの入力したユーザ認証情報に基づいて複数の画面を遷移して操作を行うような処理において、ユーザ認証情報の画面間の継承が問題となるが、ユーザ管理デーモンがユーザ認証情報を管理したまま計算機環境に常駐し続け、ユーザ認証情報にアクセスするためのユーザ認証情報識別子（ユニークかつハッキングされる恐れのない識別子）で画面間の継承を行うことにより、セキュリティとユーザの利便性の両方を確保することが可能となる。

【0070】また、ユーザ管理デーモンにユーザ情報テーブルを設け、各ユーザ固有のデータを管理することにより、従来画面情報に埋め込んで管理するしかなかったユーザデータを画面情報に埋め込むことなく画面間で継承することが可能となる。

【0071】さらに、ユーザが接続断通知をすることなくWWWゲートウェイシステムへのアクセスを終了するなどによりユーザ認証情報テーブルが過大となることを防ぐために、ユーザ管理デーモンはユーザ認証情報テーブルの最終アクセス時刻をチェックし、それが予め定められた有効期間を経過している場合には当該ユーザのユ

17

ーザ認証情報をユーザ認証情報テーブルから削除するが、ユーザ認証情報削除後にWWWゲートウェイシステムにアクセスした際に表示するユーザ認証画面に前回の操作から継続して処理を実行するための情報を埋め込むことにより、ユーザ認証後操作を始めからやりなおすことなく直前の操作から継続して処理することが可能となる。

【図面の簡単な説明】

【図１】第１の実施例における構成を表すブロック図である。

【図２】従来のWWWゲートウェイシステムの構成を説明するための図である。

【図３】ユーザ認証情報テーブルの例を説明するための図である。

【図４】ログイン時の処理の流れを説明するための図である

【図５】WWWゲートウェイシステムから既存システムの処理を実行するときの処理の流れを説明するための図である。

【図６】第２の実施例における構成を表すブロック図である。

【図７】第２の実施例におけるユーザ認証情報テーブルの例を説明するための図である。

【図８】ユーザ情報テーブル２１の例を説明するための図である。

【図９】第２の実施例におけるログイン時の処理の流れを説明するための図である。

【図１０】第２の実施例におけるユーザ情報取得処理の流れを説明するための図である。

【図１１】第３の実施例における構成を表すブロック図

18

である。

【図１２】第３の実施例における再ログインのためのユーザ認証画面生成処理の流れを説明するための図である。

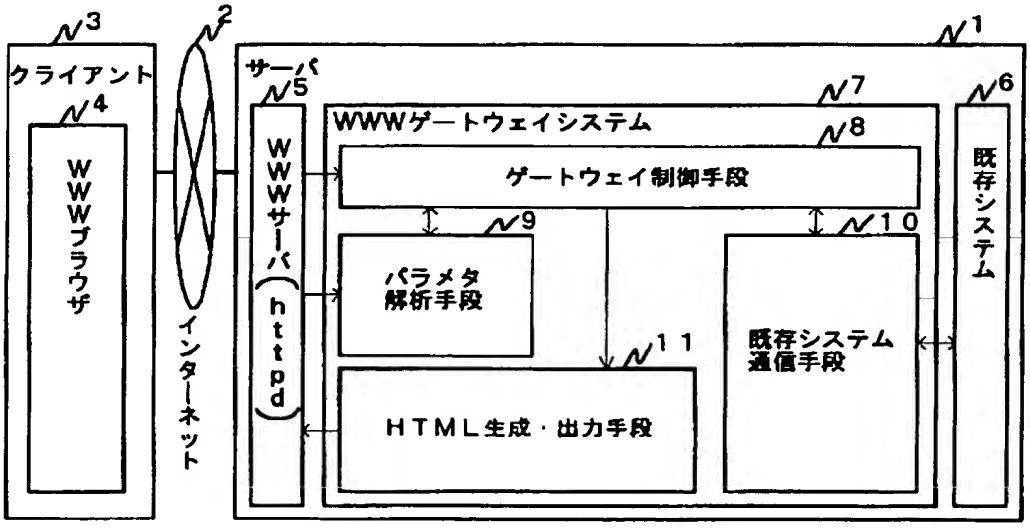
【図１３】第３の実施例における再ログイン時の処理の流れを説明するための図である。

【符号の説明】

１・・・サーバ、
２・・・インターネット、
３・・・クライアント、
４・・・WWWブラウザ、
５・・・WWWサーバ、
６・・・既存システム、
７・・・WWWゲートウェイシステム、
８・・・ゲートウェイ制御手段、
９・・・パラメタ解析手段、
１０・・・既存システム通信手段、
１１・・・ＨＴＭＬ生成・出力手段、
１２・・・WWWゲートウェイ本体部、
１３・・・ユーザ管理デーモン、
１４・・・ユーザ管理デーモン通信手段、
１５・・・WWWゲートウェイ通信手段、
１６・・・制御手段、
１７・・・ユーザ認証情報管理手段、
１８・・・既存システム問合わせ手段、
１９・・・ユーザ認証情報テーブル、
２０・・・ユーザ情報管理手段、
２１・・・ユーザ情報テーブル、
２２・・・継続処理情報埋め込み手段

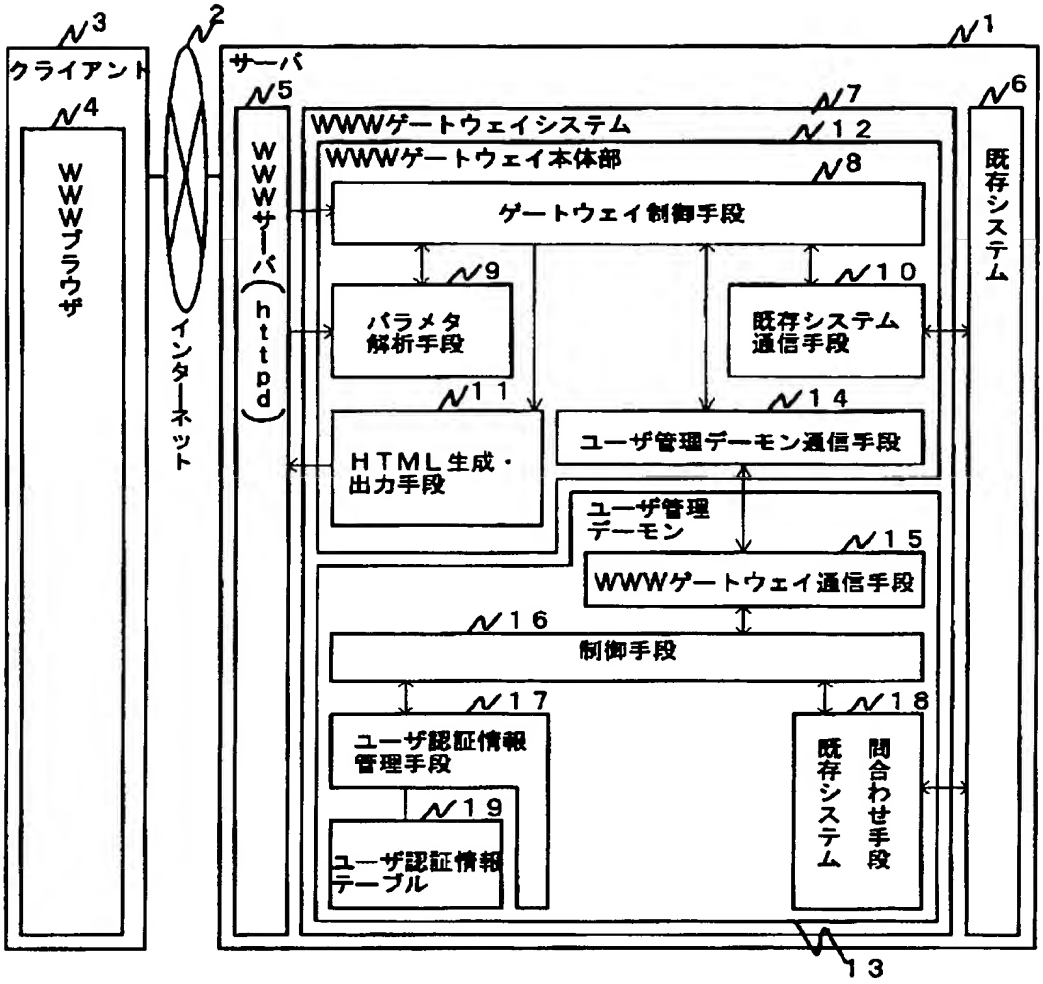
【図２】

図2



【図１】

図１



【図３】

図３

ユーザ認証情報識別子	ユーザＩＤ	パスワード	ＩＰアドレス	最終アクセス時間
97827ABC928W	AIHARA	8R6JBM7V	123. 45. 67. 890	960308170532
KU1C03860V093	AIKOU	ZZZAA0 0	123. 45. 67. 123	960308154717
OPK99UYV7Y5C	AKIYAMA	8KU=U0 HA	123. 45. 12. 345	960308165908

19

【図７】

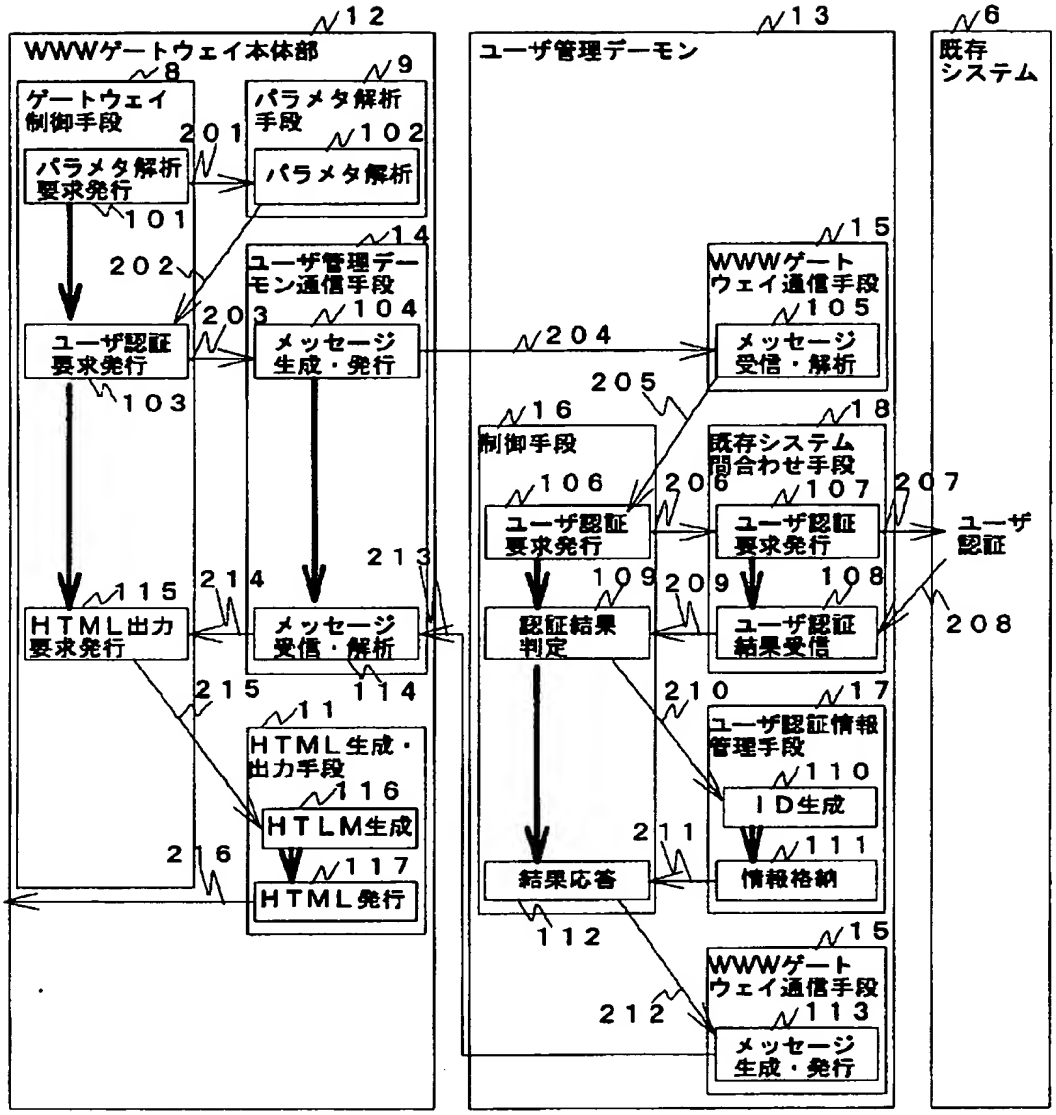
図７

ユーザ認証情報識別子	ユーザＩＤ	パスワード	ＩＰアドレス	最終アクセス時間	ユーザ情報テーブル
97827ABC928W	AIHARA	8R6JBM7V	123. 45. 67. 890	960308170532	SB7C1100
KU1C03860V093	AIKOU	ZZZAA0 0	123. 45. 67. 123	960308154717	SB7C1140
OPK99UYV7Y5C	AKIYAMA	8KU=U0 HA	123. 45. 12. 345	960308165908	SB7C1180

19

【図４】

図４



【図８】

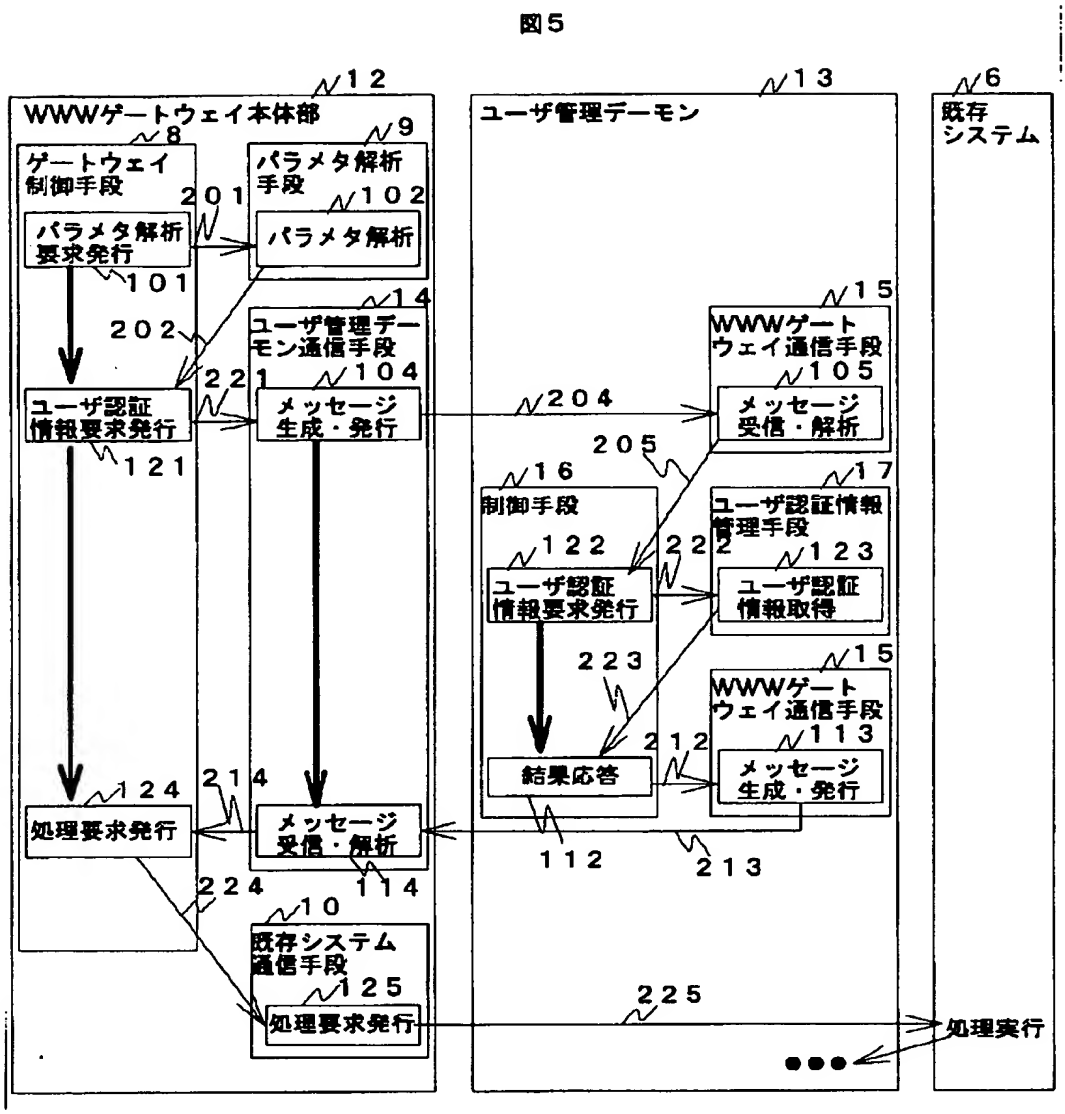
■8

21

アドレス	パラメタ1	パラメタ2
6B7C1100	XXX	ABC
6B7C1140	YYY	DEF
6B7C1180	ZZZ	GHI

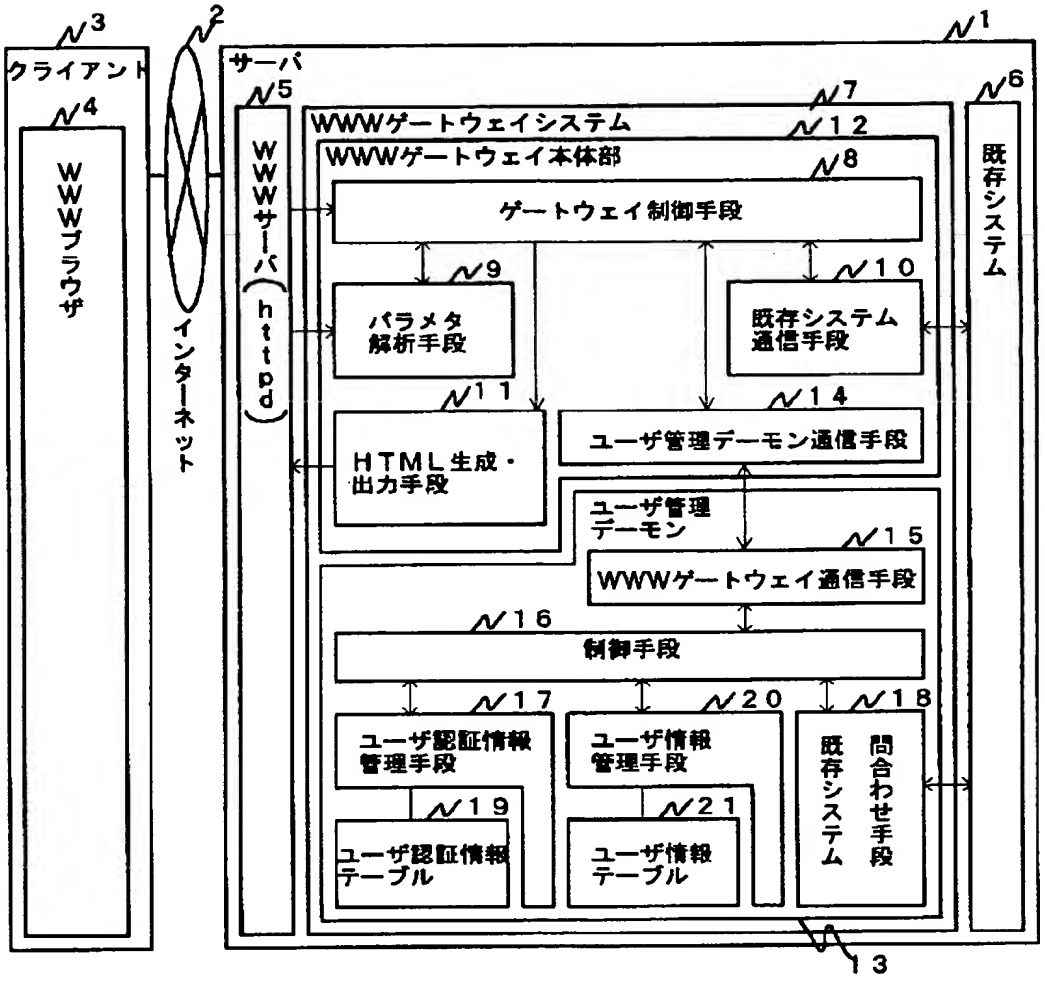
【図５】

図５


WWWゲートウェイ本体部
12
ユーザ管理デーモン
13
既存システム
6
ゲートウェイ制御手段
8
パラメタ解析手段
9
パラメタ解析要求発行
101
パラメタ解析
102
201
202
ユーザ管理デーモン通信手段
14
ユーザ認証情報要求発行
121
221
メッセージ生成・発行
104
204
WWWゲートウェイ通信手段
15
メッセージ受信・解析
105
205
制御手段
16
ユーザ認証情報管理手段
17
ユーザ認証情報要求発行
122
222
ユーザ認証情報取得
123
223
結果応答
212
WWWゲートウェイ通信手段
15
メッセージ生成・発行
113
処理要求発行
124
214
メッセージ受信・解析
114
112
213
224
既存システム通信手段
10
処理要求発行
125
225
処理実行

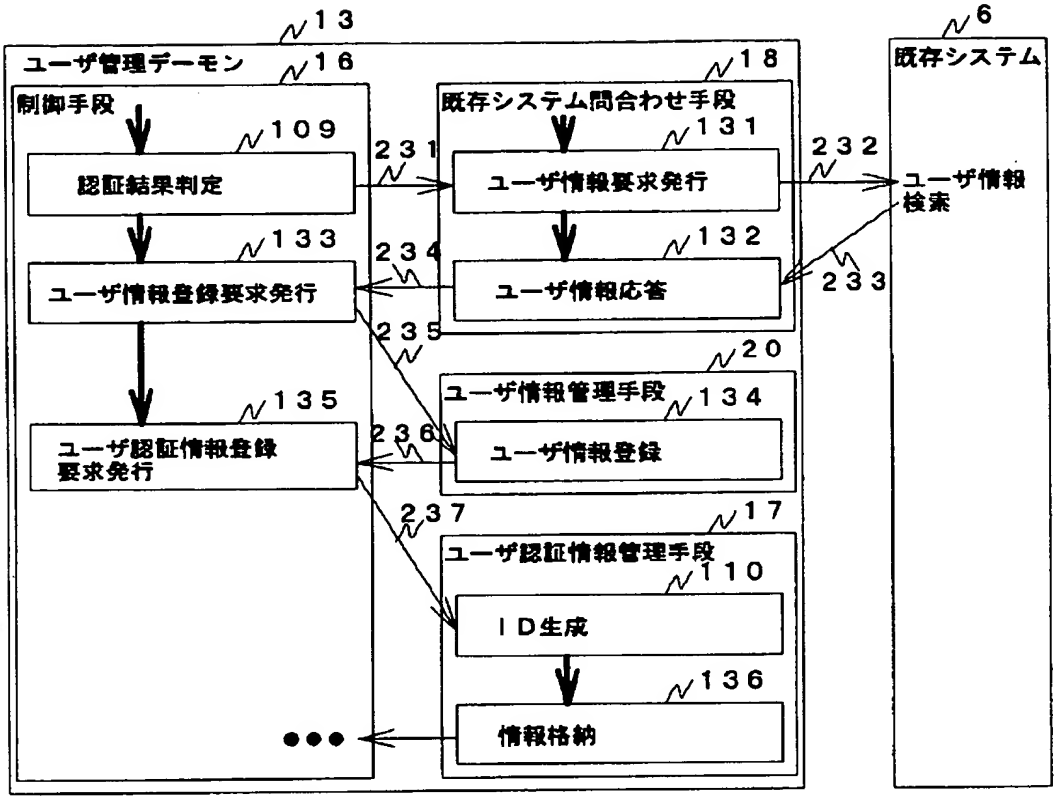
【図６】

図６


クライアント
WWWブラウザ
インターネット
サーバ
WWWサーバ(httpd)
WWWゲートウェイシステム
WWWゲートウェイ本体部
ゲートウェイ制御手段
パラメタ解析手段
既存システム通信手段
HTML生成・出力手段
ユーザ管理デーモン通信手段
ユーザ管理デーモン
WWWゲートウェイ通信手段
制御手段
ユーザ認証情報管理手段
ユーザ情報管理手段
問合わせ手段
ユーザ認証情報テーブル
ユーザ情報テーブル
既存システム
1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21

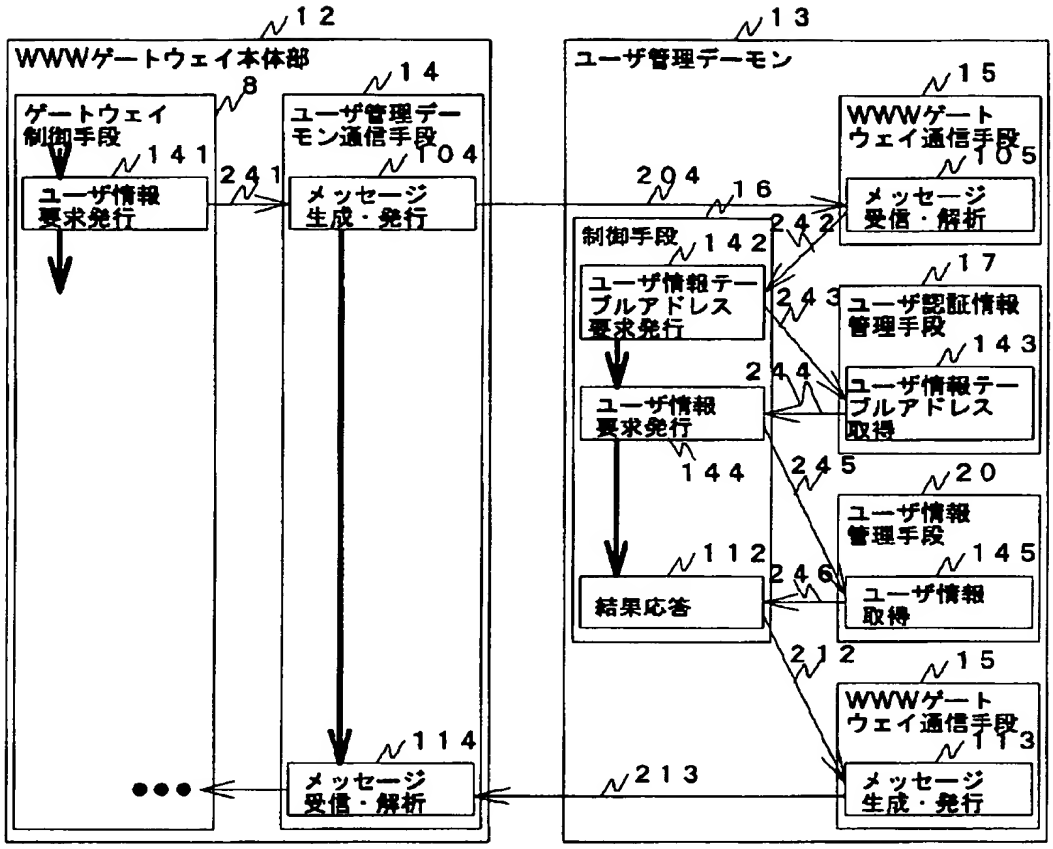
【図９】

図９


13
ユーザ管理デーモン
16
制御手段
109
認証結果判定
133
ユーザ情報登録要求発行
135
ユーザ認証情報登録
要求発行
●●●
231
234
235
236
237
18
既存システム問合わせ手段
131
ユーザ情報要求発行
132
ユーザ情報応答
20
ユーザ情報管理手段
134
ユーザ情報登録
17
ユーザ認証情報管理手段
110
ＩＤ生成
136
情報格納
232
233
6
既存システム
ユーザ情報
検索

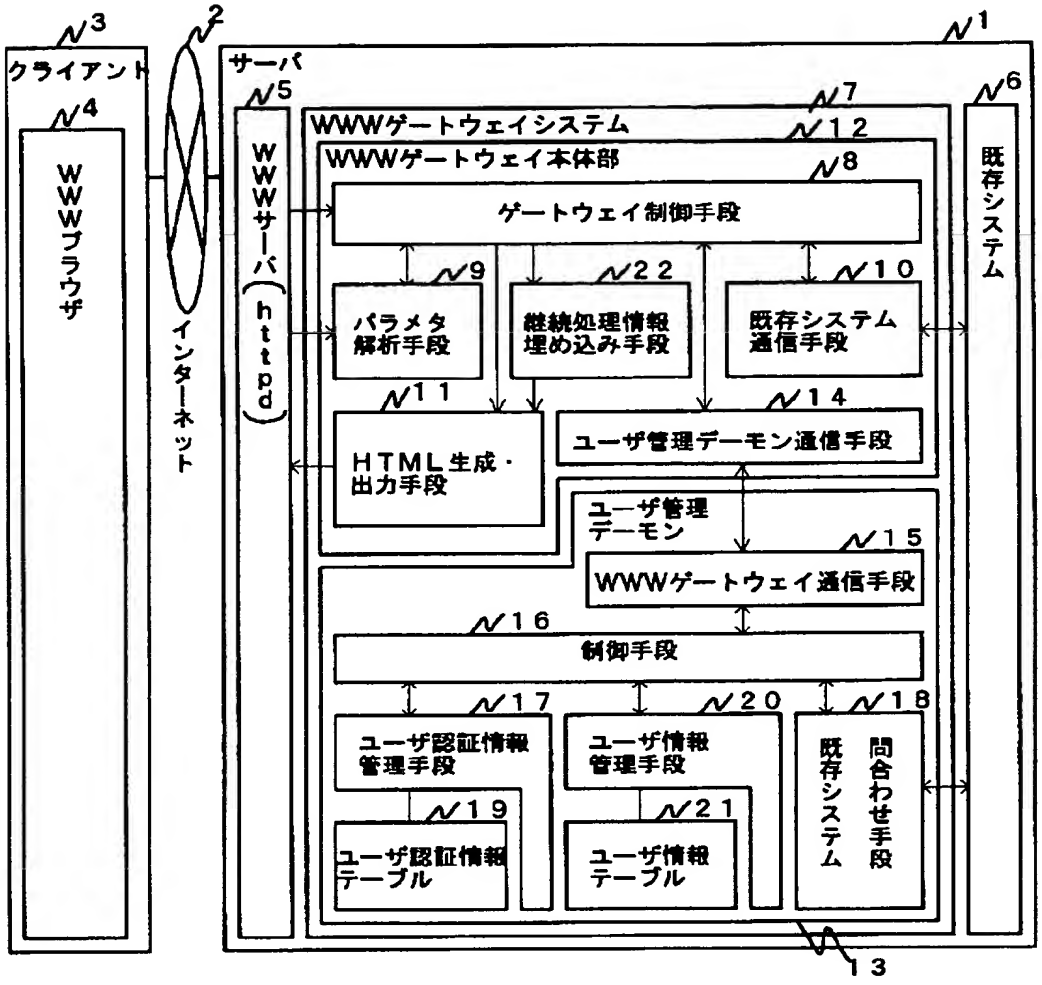
【図１０】

図１０


１２
WWWゲートウェイ本体部
８
ゲートウェイ制御手段
１４１
ユーザ情報要求発行
２４１
１４
ユーザ管理デーモン通信手段
１０４
メッセージ生成・発行
１１４
メッセージ受信・解析
１３
ユーザ管理デーモン
２０４
１６
制御手段
１４２
ユーザ情報テーブルアドレス要求発行
１４４
ユーザ情報要求発行
１１２
結果応答
１５
WWWゲートウェイ通信手段
１０５
メッセージ受信・解析
２４２
１７
ユーザ認証情報管理手段
２４３
１４３
ユーザ情報テーブルアドレス取得
２４４
２４５
２０
ユーザ情報管理手段
１４５
ユーザ情報取得
２４６
２１２
１５
WWWゲートウェイ通信手段
１１３
メッセージ生成・発行
２１３

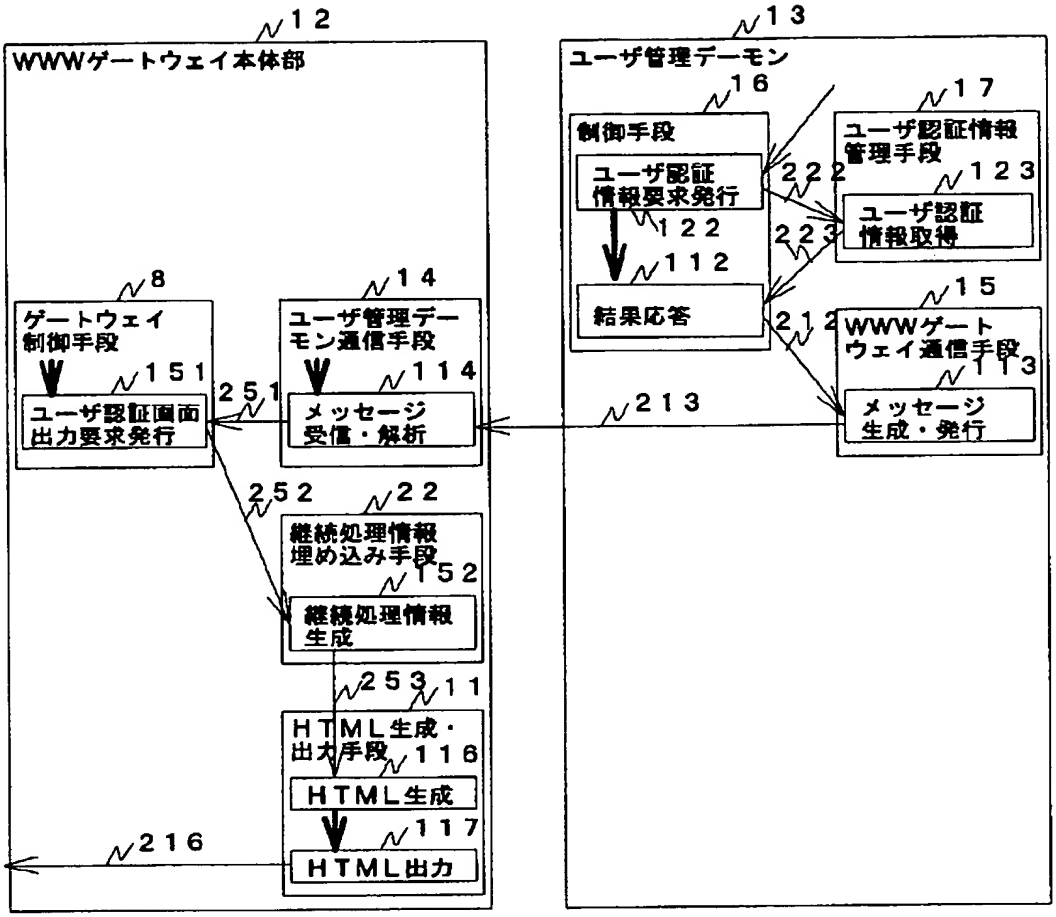
【図１１】

図１１


1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
クライアント
WWWブラウザ
インターネット
サーバ
WWWサーバ（httpd）
WWWゲートウェイシステム
WWWゲートウェイ本体部
既存システム
ゲートウェイ制御手段
パラメタ解析手段
継続処理情報埋め込み手段
既存システム通信手段
HTML生成・出力手段
ユーザ管理デーモン通信手段
ユーザ管理デーモン
WWWゲートウェイ通信手段
制御手段
ユーザ認証情報管理手段
ユーザ認証情報テーブル
ユーザ情報管理手段
ユーザ情報テーブル
既存システム問合わせ手段

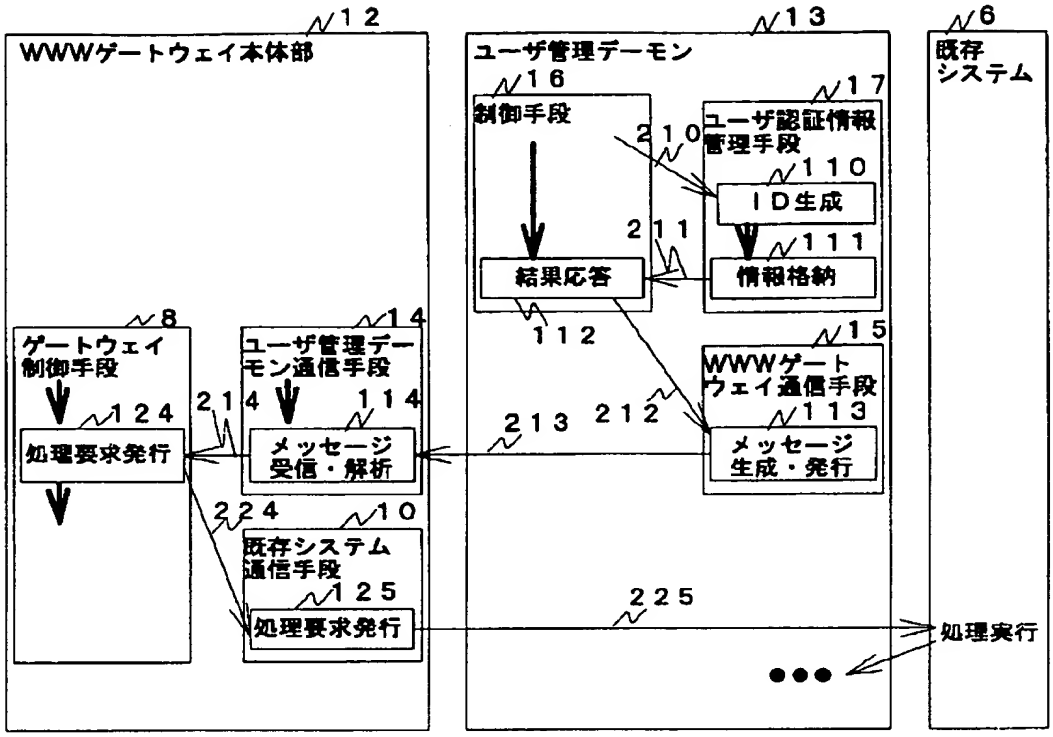
【図１２】

図１２


12
WWWゲートウェイ本体部
13
ユーザ管理デーモン
16
制御手段
ユーザ認証
情報要求発行
122
112
結果応答
17
ユーザ認証情報
管理手段
123
ユーザ認証
情報取得
222
223
212
15
WWWゲート
ウェイ通信手段
113
メッセージ
生成・発行
213
8
ゲートウェイ
制御手段
151
ユーザ認証画面
出力要求発行
251
14
ユーザ管理デー
モン通信手段
114
メッセージ
受信・解析
252
22
継続処理情報
埋め込み手段
152
継続処理情報
生成
253
11
HTML生成・
出力手段
116
HTML生成
117
HTML出力
216

【図１３】

図１３



フロントページの続き

(72)発明者　大北　龍太郎
大阪府大阪市中央区北浜三丁目５番29号
日立西部ソフトウェア株式会社内
(72)発明者　大野　広宣
大阪府大阪市中央区北浜三丁目５番29号
日立西部ソフトウェア株式会社内
(72)発明者　林　龍介
大阪府大阪市中央区北浜三丁目５番29号
日立西部ソフトウェア株式会社内
(72)発明者　多田　勝己
神奈川県川崎市幸区鹿島田890番地の12
株式会社日立製作所情報・通信開発本部内